CYBER CRIMES AGAINST CHILDREN IN VIRTUAL WORLD: AN EMPIRICAL STUDY WITH SPECIFIC REFERENCE TO KANGRA DISTRICT HIMACHAL PRADESH

A SYNOPSIS

Submitted in partial fulfilment of the requirements for the award of the degree of

DOCTOR OF PHILOSOPHY

Submitted by

SANJEEV KUMAR
(Enrollment No.: H14109)

Under the supervision of

DR. ANUPAM MANHAS
(Assistant Professor)

DEPARTMENT OF LAW
SCHOOL OF LEGAL STUDIES & GOVERNANCE
CAREER POINT UNIVERSITY HAMIRPUR
TIKKER (KHARWARIAN), BHORANJ
HAMIRPUR (HP)-176041, INDIA

2020-2021

1.1 Prelude

In the 21st century, information innovation has contacted everyone in this world. The coming of this innovation has changed how we associate with one another within no range of time. Innovation has reached each circle of human existence. Because of the improvement in innovation, we have moved from paper to a paperless world. These days Computer are utilized widely to store classified information of political, social, monetary, and individual nature, which is an advantage to the general public, and because of the blend of Computers, web and systems administration, we are setting new norms of precision, effectiveness, and speed in each field. It helps in producing profitability, inventiveness and development.

Information innovation is a mix of computers, the internet, networking (networking), and the confluence of computer organisation. Cyberspace, or the Virtual World, is a typical place created by media communications and technological advances. Through the internet, a large number of human activities have been completed. It uses association, business, marketing, banking, education, inspection, and recreational activities to become the most happening location for netizens. No one activity is unaffected by data innovation. Computer usage has spread like an epidemic in a short period, and lakhs of people regularly connect to the internet.

The internet's and computer technology's fast development throughout the world has provided mankind with a plethora of new focus points; nevertheless, it has become a badge of honour to conduct actions that are prohibited by the act. Hacking, violating copyright, psychological oppression, exploiting particular security, unlawful minimization, extortion, programming theft, and corporate monitoring are examples of how they are increasingly being used for global wrongdoings. In today's environment, cybercrime may be a brand-new kind of crime. It is defined as knowingly or deliberately engaging in illegal activities on a computer, the internet, or computer networks. Within the virtual realm of cyber space, cyber crime encompasses crime-related computers and other unlawful activity. This phrase may be made up of two words: cybercrime and crime. The virtual world is referred to as Cyber. Computers, networks, processing, global communication through the internet, and informational space are all part of it. The second word, crime, however, relates to social, economic, and political realities that have existed from the beginning of time. Crime may be defined as a legal violation for which

a penalty exists. “The criminal character of an act cannot be found by reference to any criterion other than one; is the conduct banned with penal consequences,” according to Lord Atkin. As a result, Cybercrime is described as an unlawful activity involving using a computer as a tool, a target, or both.[1]

Cybercrimes are defined by *Dr. Debarati Halder* and *Dr. K. Jaishankar* as *"Offences committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards, and groups) a Cybercrime is the most recent and, arguably, the most complex issue in the internet world.”*[2]

According to Adv Pawan Duggal, a prominent Supreme Court advocate. “*Those species of cyber crime whose genus is a traditional crime and where the computer is either an object or a subject of the criminal conduct. Any illegal conduct that utilises a computer as an instrumentality, goal, or method of propagating additional crimes falls under the scope of cyber crime*.” [3]

India is a developing nation with many new sectors, including technology, posing challenges. India went through several stages of globalisation, advancing science and technology and ushering in a new historical period. Every day, India's society evolves. Everything in India is now online, from "online commerce to online education," thanks to the arrival of computers. For college and college projects, references, history, and so on, the education industry went through a period when academics favoured Google and Wikipedia. It all began with the submission of online admissions applications. With the introduction of online education, the educational system transformed.

The initial platform for teaching will always be online, regardless of the future, but the most significant obstacle to the fast adoption of an internet education system in which information flows freely via the internet as media is "Protecting Children from the Internet." The reliance on the internet for education, interaction, and communication, with the majority of teenagers and young adults preferring to communicate exclusively through social networking sites to keep up with their peers, share notes, keep in touch

[1] Proprietary Articles Trade Association v. A.G. for Canada (1932).
[2] Cyber Crime, *available at:* https://en.wikipedia.org/wiki/Cybercrime (Last Modified May 2, 2020).
[3] Cyber Crime, , *available at:* http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Last Modified May 2, 2020).

with friends, connect with people who share a common interest, post photos online, or interact with friends in situations such as play games, chat, or discuss poor grades.[4]

Without a doubt, youth and child social networking and dependency benefits to overcome loneliness and failures in life, such as depression and the breakup of relationships, as well as enhance affection from online friends, which may have a soothing effect to defeat the situation of the tender and immature minds to overcome trauma, and also be a support in education growth and gaining knowledge. Though the widespread use of computer technology has improved the lives of many people, including children, by allowing them to be more productive at work, school, and home, criminals and predators are exploiting children and adolescents via social networking sites. Even youngsters are utilising social networking sites without knowing how to utilise them in a less ethical manner.

Facebook, Twitter, chat rooms, and YouTube are all popular social networking sites that youngsters use daily. The "United Nations Convention on Child Rights," which was adopted in 1989, was followed by the "International Labour Organization Worst Forms of Child Labor Convention," which was adopted in 1990. Still, computers and the internet were not commonplace at the time; as a result, both Conventions focused on problems affecting children. Nonetheless, the case of "Protecting Children from the Internet" was not shown. In this vein, the European Convention took the initiative in 2001 to govern and regulate the cyber domain by establishing a uniform criminal strategy to safeguard the social order from online crimes. Children and teenagers are an integral component of any society.[5]

Cybercrime refers to crimes committed via the internet or through its use. A wide range of unlawful acts is included in this category. Because of the anonymous nature of the internet, the word "cybercrime" is a catch-all term under which numerous illegal acts are included. Much unpleasant behaviour occurs in cyberspace, allowing criminals to engage in various illegal acts known as cybercrime.

Cybercrime is committed using technology as a weapon. As a result, the perpetrators of this crime are mostly technical experts who have a thorough

[4] Here's Where Teens Are Going Instead Of Facebook, *available at:* http://www.forbes.com/sites/heres-where-teens-are-goinginstead-of-facebook (Last Modified May 2, 2020).
[5] Get Safe Online Free expert advice, *available at:* https://www.getsafeonline.org/socialnetworking/social-networking-sites/UzL0woVkklQ (Last Modified May 9, 2020).

understanding of digital programmes. Cyber-terrorism, E-mail spoofing, cyber-stalking, pornography, cyber defamation, polymorphic virus, E-mail, bombing, worms, and other new cybercrimes are a few examples. If they are committed on or through the internet, a variety of conservative crimes may be classified as cybercrimes. Theft, mischief, cheating, fraud, misrepresentation, pornography, intimidation, threats, and other offences punishable by the IPC 1860 are only a few instances.[6]

No law, act, rule, or regulation has defined the exact definition of cybercrime. Despite this, the Information Technology Act of 2000 omits a definition of cybercrime. Cybercrimes, on the other hand, may be defined as crimes in which the computer is utilised as both an object and a subject in the commission of the crime, or even both. As a consequence, cybercrime includes any action that makes use of a computer as a tool, objective, or technique for committing a later crime.

The original definition of cybercrime suggests that the boundary between traditional crime and cybercrime is a shaky one. Any unlawful activity using or involving electronic media in which *mensera* is not required is considered cybercrime. Involvement at any step of the virtual cyber media, i.e., the computer, is a sine qua non for cybercrime.[7]

As defined by the United Nations, cybercrime is a kind of crime that occurs online. The "Congress on Cyber Crime Prevention and Offender Treatment" is divided into two sections:

1. "Cybercrime is a term that refers to a crime committed using a computer. It encompasses any unlawful activity involving the use of electronic operations to compromise the security of computer systems and the data they process."

2. "In a broad sense, cybercrime encompasses all computer-related offences and includes any criminal behaviour done via, or affecting, a computer system or network, including crimes like unlawful possession and providing or distributing information using a computer system or network."

In India, cybercrime is defined as the voluntary use of the internet to commit a crime, or committing a crime by committing a wilful act, omission, or commission that

[6] Anirudh Rastogi, *Cyber Law* 81 (Lexis Nexis, Delhi, 1st ed., 2014).
[7] *Id* at 82.

has an adverse effect on a person or property, or on a person's computer systems, computer network, or destruction of data, and is prosecutable under the Information Technology Act, 2000 or the Indian Penal Code 1860.[8]

Cybercrime may also include traditional criminal acts like defamation, theft, mischief, fraud, forgery, and so on, all of which are punishable under the IPC 1860. Aside from the mistreatment of computers, and systems, the internet has spawned a slew of new crimes that were unheard of prior to the advent of computer technology but are now criminal under the Information Technology Act of 2000. As a result, it would be inaccurate to state that only offences punishable under the I.T. Act are considered "cybercrime," as the Indian Penal Code 1860 also includes offences like spoofing, transmitting abusive text, E-mail, E-mail, cyber defamation, and so on.

Today, the world is confronted with a significant problem posed by the internet, the most important invention of the twenty-first century. There is little question that the internet has increased both the possibilities for humans to invent new things and the dangers they face. Almost everyone utilises cell phones, laptops, and other communication devices, as well as networks and the internet. The Digital World, often known as Cyberspace, is an environment where individuals communicate and exchange information via electronic devices. The employment of technology to cope with various everyday issues is unavoidable. In such a situation, the wise use of technological goods is essential for increased efficiency. The tragic repercussions of ignorance of its potential dangers and traps, particularly in the lives of adolescents and teens, have ensued.[9]

As the adage goes, the child is the nation's most terrific asst. It is critical to educate children about digital etiquette, as well as the dos and don'ts of the internet world. Our children will be more digitally sanitary and ethically sound in the virtual world due to this.

Kids and adolescence, children's, and youth are engrossed in the digital world primarily for teaching, schooling, teaching or education, entertainment (where they download music, dance videos, various movies, internet gaming, etc.), social communications (e-mails, Snapchat texting, chatting on Facebook, WhatsApp text Instagram text, TikTok & Snapchat videos, etc.) and online shredding (where they were

[8] *Supra* note 6 at 82
[9] *Id* at 83

downloading music, dance videos, various movies, internet gaming, etc. Amazon, Mantra, Snapdel, Flipkart, eBay, and others are examples. Children's interaction with online electronic goods has caused severe loss, even with this recommendation, according to research surveys, far beyond the warning limits. This is solely due to a lack of understanding of people's security methods in the digital world. Starting with the child, parents, teachers, government, epistemic communities, and down to the individual, everyone has a part to play in making the citizens of the digital world, especially children, resistant to cyber-attacks such as cyber stalking and bullying, kiddy porn, sexual exploitation, online harassment, fraud, morphing, and so on. These dangers do not seem to be limited to their immediate surroundings. However, they are experienced by individuals all around the globe. Because of the world the virtual world is rife with criminal activity. Everything we see, hear, and read in the digital world is inaccurate; it may even mislead us. The same motivations motivate thieves in the cyber world as they do in the real world. However, the digital realm offers great anonymity for criminals.

It is essential to teach children about safe online behaviour so that they can enjoy the benefits of the internet while also protecting themselves from the dangers of online criminals. Simultaneously, government and law enforcement agencies, the scientific community, school instructors, parents, and children must all work together to provide a safe environment for minors and to minimise and fight cyber pedophilia. It is now more important than ever to take a multi-layered strategy to deal with online hazards, which present a variety of difficulties and need more comprehensive international cooperation to find creative solutions.

William Gibson is credited with coining the term "cyberspace," which he used in his 1984 novel Necromancer.[10] As defined by Gibson, cyberspace is "a collective delusion shared by billions of legal operators worldwide, as well as youngsters learning mathematical ideas. Data extracted from the banks of every computer in the human system is shown graphically. Unfathomable intricacy, light lines are ranging through the mind's non-space, data clusters and constellations ". The term "cyberspace" entered the popular vocabulary and has since become a de facto synonym for "internet." It is wholly contained inside a computer environment, dispersed over more sophisticated and liquefied networks. As computers and the internet have increased in popularity,

[10] William Gibson, *Necromancer*, (Penguin Publishing Group, 1984).

cybercrime has become a significant problem for law enforcement agencies and civil society. Nearly 440 billion children under the age of 18 live in India, which is home to 19 percent of the world's youngsters. According to one of Ericsson's estimates, 30 million people live in cities. Mobile phones are owned by 3 million Indian children and teenagers, and parents who use mobile broadband are more likely to expose their children to technology.

Today's generation is more vulnerable to cybercrime because they use the web and online technologies extensively for everyday work and e-banking, entertainment, and education, including information, social networking, e-mails, videos, web-TV, e-shopping, home-work research, news, downloading musical videos, online gaming, movies, and other content, and so on. This often occurs in the context of social networking accounts, porn, inappropriate content, online harassment, cyber-stalking, email hacking, cyberbullying, fraud, and unwanted exposure to sexually explicit material, among other things. These dangers are not limited to their immediate surroundings; they affect individuals all around the globe. Parents and educators are unfamiliar with the dangers presented by new media devices. As a result, dealing with online hazards presents unique difficulties that need broader cooperation to find creative solutions. A comparative analysis of the many global ways to build infrastructure around secure information and communication technologies highlights the need for a multilayered approach to internet dominance in India.[11]

"A child is a person under the age of 18," according to Article 1 of the "Convention on the Rights of the Child," "unless the laws of a specific nation establish the legal age for adulthood younger." The Committee on the Rights of the Child, the Convention's monitoring body, has urged States to rethink setting the age of majority below 18 and to strengthen protections for all children under the age of 18.[12]

Children may use digital media to exercise their rights to evaluate information, play games, and express themselves freely and anonymously. By enabling communication, education, and advocacy, technology plays a critical role in empowering

[11] Saving children from legal lacuna, *available at:* http://www.savethechildren.in/component/content/article/49-newsflash/308-saving-children-fromlegal-lacuna.html (Last Modified May 19, 2020).
[12] Article 1, The Convention on Child Rights (1989).

children. It implies that youngsters are no longer reliant on adults and can speak out for themselves.

However, not every kid has the same level of access to digital media. Even with access, children face risks associated with digital media, including online safety and cyberbullying. It is important that when developing new policies or making decisions, we listen directly to children's perspectives rather than presuming what is best for them.

"The hypothetical environment in which communication across computer networks occurs," according to Oxford Dictionaries.[13]

We may describe cyberspace as the worldwide realm of interdependent and interactive networks, including the internet and other telecommunication networks, in general, without attempting a comprehensive description. In layman's terms, cyber space refers to the internet in its broadest meaning. Cyberspace encompasses anything that is linked to the internet. The cyberspace domain encompasses the vast digital body of data and information that is exchanged across different networks across the world. Whether it is your home Wi-Fi connection or your workplace phone line, every piece of digital data sent across such networks adds to the cyber-growth domains.

The realm covered by cyberspace seems to be ever-growing and ever-expanding synchronously with advancements in networking technology in the future information age. As a mirror reflection of the offline world, almost every element of our lives is creating an online counterpart. Whether for an online company or to create a virtual identity, we utilise e-commerce sites and social networking sites. Every single one of these activities adds to our online environment or personal cyber-zone. Children have taken on the job of "harbingers of the cyber age" in an ever-expanding cyberspace. In terms of numbers, the developing world accounts for about two-thirds of the global population, which is increasing by the day. Several of these new users are youngsters and teenagers; in many countries, internet users under the age of 24 outweigh the rest. Children born in the twenty-first century, which have grown up surrounded by the internet, are more intuitive and brilliant regarding digital literacy.

[13] Cyberspace, *available at:* https://en.oxforddictionaries.com/definition/cyberspace (Last Modified May 19, 2020).

A rising body of data from across the globe shows that more and more youngsters, regardless of where they are from, depend on digital tools, platforms, and programmes to learn, interact, participate, play, create, work, or socialise. With the internet and other digital technologies' advantages, there are also new developing dangers such as exposure to unsuitable material, susceptibility to offline violence, worries about excessive usage and time-killing, as well as numerous problems surrounding data security and privacy. Because recent technological and non-technical advancements have made it impossible to draw a boundary between online and offline, it is becoming more critical to examine how this dramatic shift impacts children's well-being and development, as well as their rights. When children utilise or come into touch with the Internet or any other communication medium that may be detrimental to their life, personhood, or childhood, child protection in cyberspace safeguards them from or against any perceived or actual danger/risk. It is all about making them less vulnerable to damage and hazardous circumstances. It also prevents children's social, moral, psychological, and emotional instability and suffering. It must guarantee that no kid slips through the cracks in the social security and safety net and that those who do are given the care and protection they need to re-enter the system. Online child safety is connected to all other child rights aspects. Failure to safeguard children's online rights harms all other child rights and the development of the kid's full potential. Online child protection's objective is to safeguard every child's right to access the internet or any other form of communication. It must also link children's ability for self-reliance and self-defense to the roles and obligations of their families, communities, societies, and governments.

Concept of Crime

Crimes have "always relied on the power, energy, and movement of public opinion from time to time, nation to country, and even within the same country, from decade to decade," as it has been said.[14] Crime is eternal; it has existed since the dawn of civilization and will continue to exist indefinitely. Criminals will alter their tactics as long as the company improves its security. To comprehend it better, an effort has been made to describe the notion of crime from its origins to the present day. The following are the two time periods:[15]

[14] Dr. Jyoti Rattan, Cyber Laws & Information Technology 10 (Bharat Law House Pvt. Ltd., 2014).
[15] R.C. Nigam, *Law of Crimes in India* 3 (Asia Pub. House, New York, vol. 1, 1965).

Early Concept of Crime:

Since man's fall, he has been associated with crime and criminality. Criminal crime is elusive, and it tries to stay concealed in the face of development. Numerous nations have devised various ways to fight crime, depending on the type and extent of the offence. Before the tenth century, English society conflated crimes and torts because the family bond was much stronger than the community bond, the injured party and his relatives could avenge the wrong through private vengeance and self-redress, and recourse to legal remedy was viewed as a secondary option to self-redress.[16]

At the time, the offender was required to compensate the individual who had been harmed. The amount of compensation was determined by the severity of the wrongdoing and the victim's social position. In contrast to contemporary times, the law did not force the regulation of social interactions in the early days. During the 12th and 13th centuries, the Early English culture only considered offences against the state or religion, not other crimes. During the early civilizations, there was no difference between the law of crime and the law of torts, and these communities followed the law of wrongs. As soon as an infraction is committed under current legal systems, the law is applied immediately, regardless of the wishes of the victimised party. Even yet, in early civilizations, the law was only enacted when both parties agreed to be bound by the decision. During the 18th century, often known in criminology as the "miracle reorientation" period, it was believed that only the offender could take criminal responsibility for his behaviour and that no one else, including external forces, was involved. It was apparent at the time that the idea of crime was connected to the social policies of the day.[17]

Numerous services of human life, such as agriculture, political structures, health care, medical knowledge, and basic living comforts, were rudimentary in ancient civilization, and crime was also rare. They were easy whenever they happened. They sprang from primal human desires such as lust, greed, revenge, envy, and sexual desire.

[16] Anwar M. S. Masadeh, *Combating Cyber Crimes –Legislative Approach– A Comparative Study* 6, *available at:* http://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en (Last Modified April 02, 2020).
[17] Talat Fatima, *Cyber Crimes* 61 (Eastern book company, New Delhi, 2011).

Physical force, bodily muscles, and frightening devices were also reported to be used to perpetrate crimes.[18]

Because of the differences in socioeconomic circumstances in different nations, Western countries have a significantly higher incidence of crime than India. Modernization, urbanisation, industry, scientific, technological, and civilization advancements have all contributed to an increase in crime rates. Because the danger of committing crimes is lower, scientist understands how to identify those criminals engaged in carrying out their illegal activities and escape detection. As a result, a new approach to crime and criminals was necessary to combat the new circumstances and criminals.

Modern Concept of Crime:

A functional approach to crime is a modern technique. Scientific progress, the industrial revolution, the refinement of political institutions, individual education and academic enlightenment, the waning of religious control over society, and the eroding of moral norms have all altered the criminal landscape in modern society, particularly in the information-age.

The law is constantly evolving, adding new offences to the catalogues while also amending, adjusting, and abolishing previous ones. In the realm of crime, there have been significant developments. The evolving notion of crime relies on the development of human beings in society all over the globe. Because a crime in one country may not be a crime in another, and a crime during one era may not be a crime during another. Vice versa, the idea of crime evolves differently in different nations and historical periods.

Because of economic development and wealth concentration, as well as rapid advancements in mass media, traditional crimes such as burglary, robbery, theft, prostitution, murder, rape, dacoity, and others have been transformed both qualitatively and quantitatively, resulting in the emergence of new kinds of crime.

Instead of months and years, crime waves are now tracked in hours and minutes. Its expansion may be ascribed to a variety of social and economic factors. However, there are additional reasons for its unabated growth, including its ability to provide reasonable anonymity to criminals and the impossibility of defining jurisdiction due to

[18] N.V. Paranjape, *Criminology and Penology* 4 (Central Law Publication, Allahabad, 2017).

the absence of geographical borders, which makes jurisdiction impossible to define and provides criminals with a fair chance to avoid legal action, encouraging them to go further. As a result, cybercrime is defined by all other crimes, with the addition of its vastness, anonymity, and lack of legal control regimes.[19]

Nature of Crimes:

Almost every community, in general, has a set of laws, beliefs, practises, and traditions that its members implicitly accept as helpful to their health and development. Anti-social behaviour is defined as a violation of these valued norms and traditions. Human behaviour that is forbidden by Criminal Law and punishable by the State is to be regarded as a crime. There are many instances in our society when human behaviour is prohibited by moral code, i.e. immorality, a civil wrong, i.e., and criminal law, i.e. crimes, and those that are not prohibited by any of these are not authorised by criminal law and are not erroneous. As a result, crime is a criminal offence. The following method may be used to comprehend the shifting nature of crime:[20]

Crime may be defined as an act of public wrongdoing; according to Blackstone, Crime is a social wrong. “He defines crime in two ways: first, it is an act done or omitted in violation of a public law prohibiting or commanding it; and second, it is an act committed or omitted in violation of a public law prohibiting or ordering it. We cannot accept this definition since breaches of Public Law, such as Constitutional Law and Administrative Law, are not crimes. Second, he changes his definition to state that a crime is a breach of the public's appropriate responsibilities owed to the whole community, as a whole.”[21]

The preceding definition was further amended by Stephen, the editor of Blackstone's Commentaries, who said, "*A crime is a breach of a right, evaluated in terms of the bad tendency of such violation in relation to the society at large."* As a result, Stephen and Blackstone emphasise that crimes are violations of laws that harm the community. According to Stephen, he says that *"crime is an act that is both prohibited by law and repulsive to society's moral sensibilities."*[22]

[19] *Supra* note 17 at 36-37
[20] *Supra* note 16 at 82
[21] *Supra* note 17 at 5
[22] *Id* at 6

In a second sense, crime may be seen as social wrongdoing. According to John Gillin, a crime is an act that damages society or is deemed harmful to society by a group of people with the power to impose their views and is forbidden by positive consequences. According to Raffaele Garafalo, crime is an immoral and harmful act that is seen as such by the public as a violation of so much of the moral sense as is represented by one or the other of the real altruistic feelings of compassion and pity (honesty). Furthermore, the damage must be to these emotions in the average measure in which a community has them to adapt the person to society, not in their superior and more exemplary degrees. Sutherland backs up this claim by describing crime as a sign of societal disorder. As a result, contemporary sociological criminologists consider it a social phenomena that are frowned upon by society.[23]

In a third sense, crime may be defined as "conventional wrongdoing." Crime, according to Edwin Sutherland, is defined as illegal behaviour that violates the law. It is not a crime, regardless of the degree of reprehensibility, immorality, or indecency of an act, unless the criminal law forbids it. Criminal law, on the other hand, is traditionally described as a set of particular norms about human behaviour proclaimed by political power, which is universally applicable to all members of the groups to whom the laws pertain and are enforced by the state via penalty. Polytonality, specificity, consistency, and criminal punishment set this collection of human behaviour laws apart from other authorities.

In a fourth sense, crime may be seen as a procedural error. According to Austin, an ill-gotten gain by the sovereign or his subordinate is a crime. A civil injury is an act of malice perpetrated by the wounded person or his representatives. Austin's definition was modified by Kenny, who said that crimes are wrongs having a punitive penalty that is not remissible by any private individual but is remissible only by the crown if it is remissible at all.

Fifth, a crime is defined as a breach of the law. Halsbury defines a crime as an unlawful conduct that constitutes a public offence for which the perpetrator faces legal consequences. Criminal law defines a crime as any human behaviour prohibited by law, but this does not apply to all human behaviour. As a consequence, it may be seen as a legal error. In Section 40 of IPC 1860, the term "offence" is defined as "any conduct

[23] *Id* at 8

punishable under this code." In India, any illegal acts, behaviours, or omissions that violate the law or public policy are banned and punishable under penal laws.

Concept of Virtual Space

The terms 'Virtual Reality,' 'Virtual Space,' and 'Virtual Environment' (VE) are used interchangeably to describe a computer-simulated place or environment with which users can interact via an interface. In its most advanced (and currently, putative) form, a VE would mesh seamlessly with the user's perceptions such that they would be unable to tell it apart from their perceptions of the real world.

Concept of Cyberspace

William Gibson created the term "cyber space," which he later described as a "emotive and ultimately meaningless" buzzword that could be used as a cypher (a text that has been altered in order to conceal its meaning) for all of his cybernetic concepts.

It is currently used to refer to everything related to computers, information technology, the internet, and the many Internet cultures. The cyber environment is the virtual space in which all communication and activities facilitated by information technology take place. Cyberspace is indefinable from a geocentric space. It includes intangible assets such as website, blog, social media profiles, email accounts, personally identifiable information, and reputation. Cyberspace may be likened to a global electronic community that operates in real-time and is devoid of physical borders.[24]

Cyberspace is the term that refers to the electronic medium used by computer networks. Through internet communication, individuals may interact, exchange ideas, share information, provide social support, do business, direct activities, create creative media, play games, and participate in political discussions. Cyberspace, the future frontier, is humanity's common heritage. Regrettably, some people misuse common inheritance, and the internet has become a new frontier for various illegal activities. It is currently used to refer to everything related to computers, information technology, the internet, and the many Internet cultures. Netizens are those who participate in cyberspace. The phrase is derived from "internet" and "citizen." Consequently, the term

[24] Jyoti Ratan, *Cyber Laws & Information Technology* 48 (Bharat Law House Pvt. Ctd, New Delhi, 7th ed, 2019).

"netizen" refers to anybody involved in computers, information technology, or the Internet.[25]

Definition:

"The computational medium of cyberspace is an enhancement of the communication channel between actual people; the fundamental feature of cyberspace is that it provides an environment in which numerous individuals may impact and influence one another. They came up with this idea seeing that individuals in virtual worlds want richness, intricacy, and depth."[26]

According to Webster's Dictionary, "Cyberspace is an electronic network of interconnected computers, bulletin boards, and other devices that is seen as a limitless environment that provides access to information, interactive communication, and a science fiction type of virtual reality. The hypothetical environment in which electronic communication happens or virtual reality' is what cyberspace refers to."[27]

According to Chip Morningstar and F. Randall Farmer, "The social aspects of cyberspace are more important than the technological application. The fundamental feature must be a multi-participant environment that may impact and influence one another. The computational media in cyberspace supplements the human-to-human communication channel."

"The hypothetical environment in which communication via computer networks happens," says cyberspace.

"Cyberspace is a three-dimensional representation of all the data contained in a big computer or network that a virtual-reality user may travel through."

"Cyber space is where transactions between computers take place. The word is also often used in connection with virtual reality, referring to a fictitious environment in which virtual things exist." For instance, a "computer creates an image of a structure that

[25] *Supra* note 6 at 2
[26] G.S Bajpai , *On Cybercrime and Cyber Law* 7 (Serials Publications, New Delhi, 2011).
[27] Krishan Pal Malik, *Computer & Information Technology Law* 71 (Allahabad Law Agency, Allahabad, 2014).

enables the architect to "walk" inside and see what a design might look like in cyberspace."[28]

This term's meaning has been modified many times to reflect recent technical advances. The world has seen a digital revolution and fast banking, education, social contact, companies, and national security since the creation of the internet in 1989. One of the cyberspace's most potent factors is interconnection. As it grows in scope, so does the global network's impact and efficacy. Because of the constant development of Information Technology and electronic information, cyberspace has become an integral part of our lives in a concise time. It is information that allows us to defend our country. Our country's economy is fuelled by knowledge. The information ensures that we get the products and services we need and informs and entertains us. The internet has given a forum for individuals to express their thoughts and share their perspectives. It has become an increasingly important instrument for people to do business, interact with one another, and access services while sitting at home.

People used to assist internet services in searching for directions, books, locations, and movies a few years ago. However, it has become a way of life. Every day, millions of individuals publish their personal information on Facebook. They voluntarily share it with their friends, family, and coworkers, making it more straightforward for the predator to locate its victim. People use apps for various tasks, including banking, cooking, studying, chatting, learning about the newest technology advancements, and doing business. Computers are now essential to every country's electricity grids, air traffic, significant networks, fire department dispatch system, and national defense-security. While cyberspace has many benefits, there is also a drawback to this interconnectedness. Every day, billions of individuals unwittingly connect more and more of their everyday lives into global information networks. The same reason for cyberspace's growing popularity is partly to blame for its harmful consequences. This phenomena has unique characteristics that have changed the globe in only a few years. Unfortunately, these distinguishing characteristics make it susceptible and dangerous to the general public and countries worldwide. These characteristics include digitization, anonymity, interconnectedness, decentralisation, and dependency. Cyberspace has several advantages. It allows you to communicate with others at any time and from

[28] Cybersapce, *available at:* http://en.wikipedia.org/wiki/Cyberspace#cite_note-3 (Last Modified April 04, 2020).

anywhere globally. It is growing in popularity as a respected source of information for anybody interested in learning about anything, whether they are scholars, bankers, students, lawyers, teachers, people in business, or any human being. Individuals may access breaking news, technological advancements, and research papers at the click of a button. Not only that, but individuals can immediately express their opinions with others all over the globe from the comfort of their homes. Thanks to cyberspace, everyone may now do business online, conduct financial activities, and buy online without any trouble or pain. On the internet, one may view movies, listen to music, read or create online articles, and so on.[29]

Crime in cyberspace

Cybercrime, e-crime, and digital crime are all terms used to describe computer crime and its many manifestations. All of these are crimes that involve the use or assault of computers or networks. These cybercrimes are being carried out with the intent of stealing identities and large amounts of money. "Computer crime is just regular crime carried out by high-tech computers."

A "crime in which a computer is the object of the crime (hacking, phishing, spamming) or is utilised as a tool to accomplish an offence" is classified as cybercrime (child pornography, hate crimes).[30]

"Cybercriminals may utilise computer technology to get access to personal information or company trade secrets, as well as to exploit or maliciously use the Internet. Criminals may utilise computers to communicate and store documents or data."[31]

"Computer crime, often known as cybercrime, is a kind of crime committed using a computer and a network."[32]

"Offenses committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm, or

[29] Fan Gaoyue, Threats to Cyberspace and Responses, NAPS Net Special Reports, June 13, 2013, available at http://nautilus. org/napsnet-special-reports/threat-to-cyberspaceand-responses. (Last Modified April 04, 2020).
[30] Vinod Kumar Jaiswal, *Cybercrime and Cyber Terrorism*, 12 (2010).
[31] Cybercrime, available at: https://www.techopedia.com/definition/2387/cybercrime, (Last Modified April 04, 2020).
[32] Moore, R., *Cyber Crime: Investigating High-Technology Computer* Crime, 7 (2005).

loss, to the victim directly or indirectly, through modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards, and groups) and mobile phones (SMS/MMS)."[33]

Hacking was used to getting additional information about computers and networks when they were first introduced in the 1990s. Hackers even competed against one another to see who was the most efficient and top hacker. Many commercial and government institutions, including banking and the military, have suffered due to rivalry. These hacking attempts were not taken seriously since they posed no significant danger to anybody. However, when malicious software became more prevalent, more hackers began to exploit the system, causing networks and systems to slow down. Hackers grew more dexterous and handy as time went on, and they started to abuse their knowledge and skills to benefit by abusing and suffering others for monetary gain or pure entertainment. Hackers recognised that cyberspace represents a profitable financial opportunity with a high rate of return. The danger is minimal, and given the large number of individuals who participate in online activities, they are an easy target to exploit. This is exactly what occurs in the early stages of cybercrime. Criminals were gaining access to sensitive information and data to benefit from it. The most significant element was that catching such criminals has proven difficult for authorities due to a lack of infrastructure. As a result, cybercrime has increased throughout the globe. It is now the most severe peril the world has ever faced.

Growth of crime in cyberspace

Cyber-attacks have increased dramatically all across the world. According to a study, infringement occurrences on the Indian internet rose twice between 2014 and 2015. Over the previous year, Indian organisations discovered 117 percent more experiences. In 2014 and 2015, there were 6284 such occurrences. In India, there were 2,895 infiltration attempts reported. These occurrences are increasing at an annual pace of 68 percent, according to Indian businesses. Cybercrime in India is now estimated to be at 1,49,254 and is expected to surpass 3,00,000 by 2018, with a growth rate of roughly 107 percent. 308,371,78 government websites be hacked, according to information submitted to and monitored by Indian Computer Response Team (CERT-In). In all,

[33] Warren G. Kruse, Jay G. Heiser, *Computer Forensics: Incident Response Essentials*, 5 (2002).

18,372 incidents of cybercrime have been reported, a rise of 81.9 percent over 2018. (10,098 cases). The rate of cybercrime has also risen from 8.9 percent in 2018 to 16.1 percent in 2019. Computer Related Offenses (section 66 of the IT Act) (13,814 points) had the greatest number of Cyber Crimes in 2019, accounting for 75.2 percent of all instances.[34] It has been observed that attackers are breaching computer systems in various locations around the world, employing disguised modes of operation and hidden servers to conceal the true identity of the genuine system from which the cyber-attacks are launched, making it difficult to determine the source of the cyber-attacks.

Types of Cyber crime

Cybercrime is classified into many categories depending on its severity, origin, and objectives. The following cyber crimes are classified according to the kind of victim they prey on. The next chapters will explore the effect, growth, case laws, and methods to fight this threat.

1. Individuals Targeted by Cybercrime

2. Theft of a person's property via cybercrime

3. Government-related cybercrime

4. Cybercrime is a threat to society as a whole.

Cyber Crime in Himachal Pradesh Overview

Himachal Pradesh is a mountainous and religious state. On January 25, 1971, the hilly state with altitudes ranging from 350 metres to 6500 metres became a state. Because of its high altitude, the state has a climate that ranges from tropical to arctic. In this state, the Lower Himalayan Zone, Tethys Himalayan Zone or the Higher Himalayan Zone, and they are the four zones that comprise it. Himachal Pradesh is seeing a surge in cybercrime as a consequence of the extensive use of the internet. Cybercrime is a new kind of crime that is rapidly expanding. We live in a culture that is referred to be "Technologically Civilized." Every other individual is now identified by the technologically sophisticated gadget or gazette he carries. In today's modern

[34] National Crime Records Bureau (NCRB): Crime in India 2019 *available at:* www.ncrb.gov.in (Last Modified April 04, 2020).

environment, it may therefore be stated that "living without technology is living without oxygen." Technology has made us reliant on it, and we can no longer envision or anticipate a life without the term "technology" in it. Information technology is a major field of technology. Given the fact that computers and the internet have become such an integral part of our lives, we are all a part of the cyber world, whether directly or indirectly. Each and every person who uses a computer these days should be familiar with the terms "cyberspace" and "cybercrime." Indian cybercrime has experienced a considerable rise in recent years, despite the country having the fourth highest number of internet users in the world. According to the most current statistics available, cybercrime is on the increase worldwide. However, it is true that cybercrime is not a problem that is often seen in India.

As a result, there is a false feeling of security that cybercrime is not a serious danger. However, recent events and developments have shattered our faith in this area. The terrorist assaults in Mumbai demonstrated unequivocally that the internet era has transformed human communications and the means of conducting war, bringing it from far-flung battlegrounds into the heart of our cities. Terrorists utilised the most cutting-edge technologies to carry out the assaults. As a result, these new technologies have presented new challenges to governments, law enforcement agencies, and individuals in protecting people's national and individual interests. More than 350 instances of cybercrime were recorded in the United States last year, the most majority of which were connected to email and social media account hacking, stocking via mobile phones, ATM fraud, obscene communications, and mobile phone tampering, among other things. According to Cyber Crime Branch sources, the number of complaints received was around 500; however, in some cases, the complainants did not want FIRs to be filed and were just concerned with getting their money back.

According to Satwant Atwal, Inspector General of Police (Crime) and in-charge of the state cyber unit, nearly 100 percent of cybercrime cases involved criminals operating from outside Himachal, primarily in Jharkhand, West Bengal, Bihar, and the North-East. “Tracing criminals operating from outside Himachal was a complex and difficult exercise,” he said. An additional component of the "centre for cybersecurity" would be a cyber lab, the construction of which would cost Rs 50 lakh. Forensic labs in Junga, 30 kilometres away, will be set up to conduct speech analysis and digital

forensics. This will assist to expedite the investigation and analysis of computer files, audio recordings, and digital material that has been moved outside of the country.

Indian data security council (DSCI) estimates that the nation has 355 integrated data centres, 17.4 million high-speed internet users, 24.3 million internet users, and 904 million mobile phone users, creating a major problem in combating cybercrime. In the United States, cybercrime has risen by about 40% on a yearly basis during the past few years.

According to the state's half-yearly report on cybercrime, the number of cybercrime complaints in Himachal Pradesh has increased by 88 percent this year (2020) as compared to the previous year. Between June 30 and June 30 of this year, the state cybercrime police station received 1,535 complaints, an average of 8 to 9 complaints per day, according to the data. In 2019, the station received 4 to 5 complaints per day, compared to 1 to 2 complaints per day in 2016, according to the station. In response to this year's shutdown restrictions on online use for social, governmental, and financial reasons, authorities believe that increased internet activity is one of the factors leading to the rise in criminal behaviour. Because the research does not include complaints made at traditional police stations, it is possible that the true number of cybercrime cases in the state is greater. 490 of the 1,535 complaints were concerning online financial frauds, and the police were able to get a total of Rs 15.56 lakh restored to the victims' accounts as a result of their efforts. There have been at least 501 formal complaints filed against social networking sites. From 519 in 2016 to 1,638 in 2019, the number of cybercrimes reported in the state has risen significantly in recent years, with an increase from 2016 to 2019.In the year 2019, 76 instances of cybercrime were reported in the state (IT Act alone 69 cases, IPC with IT Act 7 cases), compared to 68 cases in 2018. The instances of cybercrime recorded from 2017 to 2019 are shown in Chart-1. According to the statistics from the past three years of crime review reports issued by the Himachal Pradesh State Crime Bureau, the cyber crime against minors in Kangra district in Himachal Pradesh continues to grow. Kangra District is a Himachal Pradesh district in the Kangra area, having its administrative seat in Kangra city. According to the 2011 census, the district covers 5739 square kilometres and has a population of 15,10,075 people, comprising 7,50,591 men and 7,59,484 women (females). The sex ratio in the district is 1012 (females for every 1000 men). Hinduism (96.76 percent) and Islam (1.31 percent) are the two most common faiths in the area. The district's literacy rate is 85.67 percent for

people, 91.49 percent for men, and 80.02 percent for women (females). Hindi (95.18 percent), Punjabi (2.09 percent), and Tibetan are the most commonly spoken languages (0.81 percent). For the 2017-2018 fiscal years, the labour force participation rate was 54.30 percent. Agriculture is the district's primary source of revenue, with a per capita income of Rs. 86,637. For the year 2018, the district's crime rate was 171.45 percent. The overall cultivated area is 239,922 hectares, with a forest area of 2354.19 square kilometres (2019).[35]

1.2 Problem Profile

As we have seen, India has embarked on a path to become a "digital India" to improve governance and transparency. India is a developing nation, and technology is critical to achieving the aim of a digitally empowered society. Technology adoption is growing; in this case, India's children and young have never utilised it. According to many polls and estimates, India is the world's second-largest smartphone user, which is both good news and cause for worry. People utilise social networking sites for various purposes, including information, communication, messages, letters, court summonses, and e-mails. Modern technology makes all school and college courses online, even during lockdown time. Even young toddlers have a good understanding of how to utilise technology.

On social networking sites, the kids are playing games, talking, forming groups, video conferencing, creating TikTok videos, and engaging in a variety of other activities. A small number of people, especially children and teenagers, utilise technology for illegal purposes to vent their emotions, harass, threaten, stalk, and damage others via the internet, using gadgets such as mobile phones, laptops, computers, pen drives, and other similar devices. Almost every school-aged child today has access to social media. However, strangely, only a small percentage knows how to manage their personal information. They put themselves at risk of all sorts of cyber harassment by disclosing intimate information about their personal lives online.

The advancement of the internet has both good and bad consequences in the form of cybercrime that affects everyone, even children. In every case, a child is victimised,

[35] *Available at:* https://www.datanetindia-ebooks.com/District_Factbook/Himachal_Pradesh/Kangra (Last Modified May 09, 2020).

and cybercrime that impacts them must be treated seriously. Hacking, spam, viruses, credit card fraud, pornography trafficking, posting a ludicrous picture, sending counterfeit e-mails to obtain sensitive information, misusing sensitive information, digital piracy, financial fraud, counterfeit products, altering data for profit or political goals, and invading privacy by trying to steal identities are all examples of cyber terrorism attacks. Using fictitious identities in online chat rooms, criminals can convince victims to meet in person, resulting in juvenile sexual exploitation such as sex smuggling and sex tourism. The children have no idea whom he or she is conversing with. It is only when they meet in person that they realise their error and see a person who may be an older guy in his 40s or 50s with whom they were talking. When their awful photos are shared online, many youngsters commit themselves. Because they are scared of causing further problems, children frequently avoid informing their parents or anybody else about their errors.

This study will look at different technological and legal loopholes in Indian cyberspace that must be addressed as soon as possible. This research will examine the technological and legal issues of protecting children in cyberspace and ensuring their rights.

1.3 Literature Review

A Handbook and Guide to Evaluation and Treatment by Cristiano Nabuco de Abreu and Edited by Kimberly S. Young[36]

Internet addiction is a relatively new phenomena, and although research has shown that it has grown into a significant health-care concern, a complete understanding of the problem is still in its early stages. Internet Addiction: A Handbook and Guide to Education and Treatment is the first complete compilation of current research to address this problem, and it was published in 2010. In this book, the author discusses the effects of Internet Addiction on one's health and social life. There was also discussion of addiction evaluation methods and different types of psychiatric therapies for the disorder.

[36] Kimberly S. Young & Cristiano Nabuca de Abreu, *Internet Addiction : A Handbook and Guide to Evolution and Treatment* (John Wiley & Sons,Inc., 2011).

Bullying in Different Contexts Edited by Claire P. Monks and Iain Coyne[37]

This book dealt with bullying. Bullying and abuse among children on the playground are often associated with aggressive behaviour, but bullying and abuse may occur in a variety of different social settings. Bringing together renowned worldwide academics for the first time, Bullying in a Number of Contexts examines these behaviours in a variety of settings such as preschool, school, family, foster care, prisons, the workplace, and cyberspace. The book is divided into four sections. The writers give context for the various situations and explain the effect and kinds of interpersonal violence, as well as the characteristics of individuals who are engaged. The results from each setting are compiled in the last chapter, which concludes the parallels and variations in the behaviours, risk factors for participation, and theoretical methods to explaining bullying. The authors want to demonstrate how research from various contexts may influence our overall views of the bullying observable fact.

Computer Forensics and Cyber Crime an Introduction by Marjie T. Britz[38]

A thorough examination of cyberspace and computer investigations is included in the textbook. The author sets the scene for the various settings by going through a number of other topics that are important to both investigators and researchers. In this book, author will cover about hacking, networks, intellectual property theft, the Internet, (you know, that time someone left the company and took the keys to the kingdom with them), other types of computer-related fraud and, most importantly, terrorism, organised crime, and sexual crimes in a technological society, as well as how computers and computer investigation relate to these issues. The author also covers the historical, technological, legal, and specialised topics that today's computer forensic analysts, investigators, and experts need to be acquainted with in order to do their jobs effectively.

Digital Evidence and Computer Crime Forensic Science, Computers and the Internet by Eoghan Casey[39]

Fundamental ideas and legal problems related to digital evidence and computer crime are split into five sections in this book. Computer Science, according to the book's

[37] Claire P. & Monks Iain, *CoyneBullying in Different Contexts* (University Press, Cambridge, UK, 2011).
[38] Marjie T. Britz, *Computer Forensics and Cyber Crime An Introduction* (Pearson Education Inc, UK, 2013).
[39] Eoghan Casey, Digital *Evidence and Computer Crime Forensic Science, Computers and the Internet* (Published by Elsevier Inc, UK, 2011).

author, offers the technical information required to comprehend particular elements of digital evidence. Forensic Science provides a broad framework for evaluating all types of digital evidence. Behavioural Evidence Analysis is a systematic technique of combining specific technical knowledge with broad scientific methodologies in order to better comprehend criminal behaviour and motive. The use of knowledge by criminals, both violent and white-collar, to aid their crimes and avoid fear has created new challenges for attorneys, courts, law enforcement officials, forensic examiners, forensic analysts, and corporate security professionals. Because of the massive amounts of narcotics, child pornography, and other illegal items that are being trafficked on the Internet, the United States Customs and Border Protection Cyber Smuggling Centre has come to view every computer in the United States as a potential port of entry for illegal goods.

Grooming'and the Sexual Abuse of Children Institutional, Internet, and Familial Dimensions by Anne-Marie Mcalinde[40]

The creation of sexual grooming, political disputes, and the evolution of policy and legal responses in the Republic of Ireland or United Kingdom is all examined in this book. It provides enlightening statistics on the type, forms, and degree of grooming, demonstrating the seriousness of the problems confronting lawmakers, politicians, and, not least, experts on the ground. The last section of the book offers intriguing reform suggestions that go beyond criminalization to propose a public health strategy based on social and institutional initiative aimed at the dual goals of prevention and defence. Machined explains how such a shift in grooming philosophy might be accomplished. Nonetheless, she recognises the ongoing challenges, not least in raising awareness of the frequency of sexual offending against children both inside and beyond the family unit. As a result, she adds to more important discussions regarding sexual crime, child protection, risk assessment and risk management, penal populism, the media's role, and penal politics in general.

Gregory S. Smith's "*How to Protect Your Children on the Internet: A Roadmap for Parents and Teachers"* is a guide for parents and teachers on how to keep their children safe online.

[40] Anne-Marie Mcalinde, '*Grooming' and the Sexual Abuse of Children Institutional, Internet, and Familial Dimensions* (Oxford University Press, UK, 2012).

How to protect your children on the Internet : A roadmap for parents and teachers by Gregory S. Smith[41]

This book is intended for parents of children aged 8 to 17 who have access to the Internet, as well as for the educators who work with these youngsters. It is possible that the Internet and the technology that allows for online interaction and access to a wide range of content will be harmful to youngsters. The risks are genuine, and today's parents are faced with many perils that they are unaware of. Simply said, the goal of this book is to raise awareness about the dangers of the Internet by revealing some recent real-world catastrophes, as well as to provide a practical strategy and road map to assist parents safeguard their children from the dangers of the Internet.

A Practical approach to Cyber Laws by Mani [42]

This book addressed the Indian legal framework for ensuring the safety of Indian citizens in cyberspace. It was highly worried about different cyber crimes, digital evidence admissibility, and judicial interpretation of cyber cases.

Cyber Laws by Dr. Gupta & Agrawal[43]

This book is a great resource for various cybercrime case studies in India. The Information Technology Act of 2000, as well as its numerous sections, norms, and regulations, were also addressed.

Cyber Law : Indian & International Perspective By Aparna Viswanathan[44]

This book covered a broad range of topics in cyber law, including data security, intermediary liability, obscenity and child pornography, and cloud computing, from both an Indian and international perspective. It addressed, above all, the right to privacy in the context of internet.

[41] GREGORY S. SMITH, *How to Protect Your Children on the Internet A Road Map for Parents and Teachers* (Praeger Publishers, USA, 2007).
[42] Mani, *A Practical Approach to Cyber Laws* (Kamal Publishers, 2012).
[43] Dr. Gupta & Agrawal, *Cyber Laws* (Published by Premier Publication Company, 2008).
[44] Aparna Viswanathan, *Cyber Law : Indian & International Perspective* (2015).

Criminal Court Handbook by Haresh A. Shukla[45]

The Indian Penal Code, 1860, The Code of Criminal Procedure, 1973, and The Indian Evidence Act, 1872, were all extensively covered in this book, with the most recent changes and comments.

Cyber Crimes, Electronic Evidence and Investigation: Legal Issues by Vivek Sood[46]

In his book, Vivek Sood proposes a number of methods for combating cybercrime. He claims that since cybercrime is a technology-based crime, the appropriate response is security technology. Some of the most widely used security technologies are firewalls, anti-virus software, and anti-intrusion systems. He came to the conclusion that the greatest cybercrime slogan is "*defend yourself."* To confront cybercriminals and bring them to justice, he believes that real collaboration between law enforcement authorities inside the country and across countries is also required. In addition, he advocates for the reinforcement of expatriation accords and their execution as necessitate in the digital era.

Cyber Security, Law and Digital Intelligence by Mark Johnson [47]

In his book, Mark Johnson discusses the problem of overdependence on technology, particularly the internet and information technology. As a result of this increasing reliance, cyber dangers have raised, and they continue to rise with each passing day. This book examines the significance of recognising current cybersecurity risks in order to successfully respond to unprecedented difficulties, emphasising that a cybersecurity framework and digital skills are required tools to effectively respond to this issue.

Cyber Security and Cyber-war by P.W. Singer and Allan Friedman [48]

P.W. Singer and Allan Friedman highlight the significance of cyberspace, as well as its good and negative effects on society, in their book. This book offers insight into the aforementioned study, which was done to provide light on current cybercrime problems. This book also covers cyber security problems such as cybercrime and online

[45] Haresh A. Shukla , *Criminal Court Handbook* (Kamala Publication House, 2013).
[46] Vivek Sood, *Cyber Crimes, Electronic Evidence and Investigation: Legal Issues*, (2010).
[47] Mark Johnson, Cyber Security, Law and Digital Intelligence, (Gower Publishing Ltd. 2013).
[48] P.W. Singer & Allan Friedman, Cyber Security and Cyberwar, (Oxford University Press ,2014).

freedom, as well as politicians defending their country against new kinds of assault while planning new cyber battles with their neighbours to gain a strategic edge.

Cyber Security, Cyber crime and Cyber Forensics:--Applications and Perspective by Raghu Santanam, M. Sethumadhavan and Mohit Virendra[49]

In this book, Raghu Santanam, M. Sethumadhavan, and Mohit Virendra discuss different methods for protecting and developing cyberspace. This book covers a wide range of cyber security topics, including how to utilise technological and social tools to use information technology infrastructure in the safest possible manner without jeopardising its very survival.

Cybercrime - A Clear and Present Danger: The CEO's Guide to Cyber Security by Roger W. Smith[50]

In his book, Roger W. Smith eloquently demonstrates how hackers steal information online, resulting in annual losses of millions of dollars. This book outlines a number of steps that businesses and people may take to protect their personal information. Cybercrime is evolving at the same rate as the digital world.

Cyber Crime in India: A Comparative Study by Dr. M. Dasgupta[51]

As a result of the rapid advances in information and communication technology (ICT) as well as its increasing significance in the areas of data storage, reception, and sharing across the globe, M. Dasgupta's work highlights the need for greater security in the information and communication technology (ICT) field. This book explains the need of establishing a cybersecurity framework in order to evaluate and manage the increasing cybercrime problem, as well as risk management and control using information assurance machinery.

Cyber Laws by Justice Yatindra Singh [52]

The concept of intellectual property, such as trademarks, copyrights, and patents, is explained by Justice Yatindra Singh in his book Cyber Laws. Mental production

[49] Raghu Santanam, M. Sethumadhavan & Mohit Virendra, Cyber Security, Cyber crime and Cyber Forensics:--Applications and Perspective, (Idea Group inc.,2010).
[50] Roger W. Smith, Cybercrime - A Clear and Present Danger: The CEO's Guide to Cyber Security, (Create Space Independent Publishing Platform; 1 Edition, 2014).
[51] Dr. M. Dasgupta, Cyber Crime In India A Comparative Study, (Eastern Law House, 2014).
[52] Justice Yatindra Singh, Cyber Laws, (Universal Law Publishing Co. Pvt. Ltd., 2010).

property such as innovations, literary and artistic works, symbols, names, images, and designs, as well as the proprietary rights in them, are covered by intellectual property rights. To study cyber laws in detail, he has studied the science behind new emerging technologies to try to address legal issues. He is mentioned the concept of digital signature, electronic signature, and all relevant provisions pertaining to them, including authentication and recognition of it, all through the use of light on the electronic governance set forth in the Information Technology Act, 2000 as amended by Amendment Act, 2008. His studies revealed that a new class of people, called intermediates, assist the transfer of information via the use of physical infrastructure. In addition, his administration recognises and punishes all cybercrimes as per the Information Technology Act of 2000, as amended by the Amendment Act of 2008. He has discussed the Napster case's legal decisions, as well as IP rights violations on the internet, in-depth. Additionally, he addressed the United States Supreme Court's ruling in the "Re Bilski Case," which has created a debate on whether computer software qualifies for patent protection. This book includes a new chapter which covers the 'Invention and Proprietary Information Agreement (IPIA)' and all of its provisions.

Cyber Laws & Information Technology by Dr. Jyoti Rattan [53]

Cyber crime is a complex and wide-ranging issue, with numerous unique concepts, ideas, and theories that can be addressed in depth in Dr. Jyoti Rattan's book "Cyber Laws & Information Technology." The book begins with a discussion of the evolution of computers, which includes their generation, types, components, characteristics, advantages, and disadvantages. This is followed by a description of the emergence of information technology, which includes the internet, networks, and cyberspace. She is also thinking about the concept of netizens via light. Everything in the book has been illustrated using real-life examples to help the student comprehend the information more easily. She has studied the jurisdiction of the internet in both civil and criminal cases, and has written a book on it. For her, cybercrime is the use of a computer to perform any illegal activity that traditionally occurs on a computer. The primary aim of cybercrime is to get a computer or destroy data.

[53] Dr. Jyoti Rattan, Cyber Laws & Information Technology (Bharat Law House Pvt. Ltd., 2014).

Cyber Laws by Dr. Gupta and Agrawal's[54]

For any novice, this book is a great source of knowledge. It began with computer basics and progressed to encryption technology, contractual and evidentiary elements of cyber legislation, and intellectual property rights in the cyber era, cyber consumer protection, and so on. It mostly focuses on cybercrime and the Indian Information Technology Act, 2000's flaws.

Digital Security: Cyber Terror and Cyber Security (The Digital World) by Ananda Mitra[55]

Ananda Mitra discusses all of the drawbacks of extensive internet use on a global scale in his book. It has also highlighted different computer crimes and kinds of cyberattacks that are being perpetrated across the globe, as well as their global effect. This book shows how computers have a role in both committing and preventing crimes.

Essentials of Cyber Security by Dr. Gurpreet S Dhillon[56]

Gurpreet S Dhillon explains in his book the many challenges that a nation must overcome in order to protect its cybersecurity architecture. Because of its financial and infrastructural capabilities and resources, the government plays a major role in reducing the increasing risks of cyber incursions, according to this book. Online scams, cyberstalking, cyberbullying, virus assaults, malware attacks, cyber forensics, and cyber terrorism are among the numerous cybercriminal behaviours covered and explained in this book.

Indian National Cyber Security Policy- A Legal Analysis by Pavan Duggal [57]

Pavan Duggal examines India's National Cyber Security Policy, which was released in 2013. This book discusses the many aspects of India's cybersecurity vision and how it advises moving ahead in strengthening and conserving cybersecurity in India. From a legal standpoint, the book examines India's Cyber Security Policy. This book examines the advancements achieved by the Indian Cyber Security Policy as well as

[54] Dr. Gupta & Agrawal, Cyber Laws , (Published by Premier Publication Company, 2008).
[55] Ananda Mitra. Digital Security: Cyber Terror and Cyber Security (The Digital World), (Chelsea House. ; 1 Edition (1 May 2010).
[56] Dr. Gurpreet S Dhillon, Essentials of Cyber Security, (Paradigm Books, 2014).
[57] Pavan Duggal, Indian National Cyber Security Policy- A Legal Analysis, (Saakshar Law Publications, 2015).

some of the policy's shortcomings. This book analyses the Indian Cyber Security Policy for a layperson to have a more complete picture of India's cybersecurity situation.

Information Technology: Law and Practice by Vakul Sharma[58]

Cyber laws related to information technology, as mentioned in Vakul Sharma's book "Information Technology: Law and Practice," are addressed in this text. His work is easier to understand due to the abundance of real-world examples included in his writing. He has done an extensive research on the question of jurisdiction in the world of the internet and all the offences that are criminal under the Information Technology Act. in order to explain these principles and decide on jurisdiction on an international level, he has addressed numerous concepts including the territorial principle, nationality, protective principle, passive personality principle, effects principle, and universality principle. For the topic of extradition for cyber offenders, he has emphasised on the problematic subject of jurisdiction regarding cyber crimes. He has done a wonderful job by analysing the court decisions in order to ascertain the real purpose of the legislation behind the passage of Act. To assess and comment on the duties and capabilities of the Controller of Certifying Authorities, Adjudicating Officers, and Police officers under the Information Technology Act, he has performed a thorough examination.

Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India by Dr. Vishwanath Paranjape[59]

In his work, Dr. Vishwanath Paranjape points out that with the speedy development of computer technology and the internet over the years, the problem of cybercrime has grown to enormous dimensions and has become a worldwide concern. He has advocated for international collaboration in the fight against cybercrime. He has covered a wide range of national and international conventions, conferences, summits, and other events related to cybercrime and municipal cyber laws in nations such as the United Kingdom, the Germany, United States, Japan, Canada, China, Australia, India, and France.

[58] Vakul Sharma, Information Technology: Law and Practice, (Universal Law Publication, Co., 2010).
[59] Dr. Vishwanath Paranjape, Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India, (2010).

Law relating to Computers, Internet and Ecommerce: A Guide to Cyber Laws and the Information Technology Act, 2000 by Nandan Kamath[60]

Nandan Kamath's work addresses the expanding field of "electronic evidence" in the context of cybercrime, which is a rising topic of interest. Other topics he researched included the admissibility and authenticity of electronic records, the burden of proof in cybercrime, and the creation and impact of such evidence. He also studied other topics such as video-conferencing, forensic computing, and other aspects of the best evidence rule, among others.

Protection of Children on Internet By Karnika Seth[61]

In the past two decades, the development of information technology in India and other countries has been remarkable. It has resulted in a shift in the way we communicate, engage, do business, and seek and exchange information and expertise on the internet. This book focuses on how the Internet affects children and why it is a major issue for law enforcement, internet service providers, parents, educators, and children themselves.

The Internet- By Douglas E. Comer [62]

The Internet book takes a non-technical look into computer networking and the Internet. It describes how computers communicate, what the Internet is, how it works, and what you can do with it. The most important aspect is that everyone can comprehend the many ways in which the Internet has the ability to alter our lives.

1.4 Objectives

1. To study the existing legal framework and to find out drawbacks in relation to children.
2. To examine the magnitude and reasons for cybercrime against children in Kangra district Himachal Pradesh.
3. To explore the legal possibilities for reducing cybercrime against children, particularly Kangra district Himachal Pradesh.

[60] Nandan Kamath, *Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000*, (2009).
[61] Karnika Seth, *Protection of Children on Internet*, (Universal Law Publishing Co. Pvt. Ltd, 2015).
[62] Douglas E. Comer, *The Internet*, (Eastern Economy Edition, 2001).

1.5 Hypothesis

It is hypothised that cyber crime against children particularly kangra district Himachal Pradesh is increasing. It is further hypothised that there is a gap between the laws framed to protect children from cyber crime and its implementation.

1.6 Research Methodology

In the current study, the research technique is based on both doctrinal and non-doctrinal research. Its nature is descriptive and analytical. The study relies on both primary and secondary data sources. Relevant material collected from primary source, substantive and procedural pieces of legislation, as well as through questionnaires developed by the researcher for various stakeholders for the current research, and secondary sources include crime reports, journals, books, case laws, and internet surveys, among others. The study's findings will be based on statutory provisions and case law.

1.7 Universe of Study

India is the world's third-largest internet user and second-largest mobile user. Children are declared a tremendous national asset in the National Policy for Children of 1974. Nearly one-fifth of the world's children live in India. There are about 440 million children in the nation under the age of 18. Child safety in cyberspace has become the most serious issue globally as a result of technological advancements, and the majority of countries have made “Child Safety in Cyberspace” a top national priority. With their digital devices, technology offers great leverage to children and youngsters. With their digital devices, technology gives children and adolescents enormous ability to accomplish anything in cyberspace. Children's curiosity and lack of technological understanding lead them to unanticipated hazards and make them potential cyber-victims. Children are more susceptible than ever before because to the anonymity of internet. To address this problem, major nations have already begun to change their laws, technological infrastructure, and international collaboration. They are increasingly worried about children's privacy in cyberspace, and all stakeholders must make their best efforts to this end in himachal pradesh. As a result, different issues must be evaluated using comparative analysis.

1.8 Chapterisations

To keep the present study shall be divided into eight chapters viz;

Chapter-1 is titled as **"Introduction"** it will cover a brief introduction to the topic of the thesis. It also includes the concept of crime, cybercrime, and cyberspace and the impact of IT on children. It further discussed the problem profile, Literature Review, Objectives, Hypothesis, Research Methodology, Universe of study, and chapterisation.

Chapter-2 is titled as **"Historical Perspective"** it will cover the historical perspective of cyber crime and establishes a connection between history of computer and internet with the tremendous increase in the threat of cyber crimes. It will cover cyber crime and its classification. It analyses the definition of cyber crimes as given by renowned authors and jurists. The researcher has explained the nature, scope, characteristics, essential elements, and classification of cyber crimes on global basis and also the factors responsible for cyber crimes. The researcher also discuss the major crimes like Cyber Pornography, cyber stalking, cyber terrorism, hacking, stealing personal data, cyber crime related to finance etc.

Chapter-3 is titled as **"International Legal Framework"** it will cover the international legal framework for the protection of children which includes the various conventions.

Chapter-4 is titled as **"Constitutional and Indian Legal Framework"** it will cover different initiatives taken by India to addressed child protection issue. It further discussed about the constitutional safe guards for children and various other statutes dealing with children.

Chapter-5 is titled as **"Victimization of Children under Cyberspace**" it will cover different threats and modes of victimizations for the children in cyberspace. It also discussed Indian landscape of the information technology and different cyber-crimes against children.

Chapter-6 is titled as **"Judicial Approach"** This chapter will cover the judicial approach on the issue of cyber crime against children in India. Thus this chapter will cover the various judgments of the apex court and other lower courts on the issue of the children protection under cyberspace in India.

Chapter- 7 is titled as **"Results and Discussion"** is devoted to an empirical analysis of cyber crime in the district Kangra Himacal Pradesh in the form of response collection from school going children and teachers. This chapter will describe the results of the study undertaken by the researcher. The analysis of the fifth chapter will help to draw certain important result and discussion.

Chapter-8 is titled as **"Conclusion and Suggestions"** it will concludes the study with different assessments and suggestions about developing and formulating child protection related laws, rules and policies in the context of child protection in cyberspace. It further discussed the various stakeholders role in protecting children in cyberspace and recommends number of measures and strategies to protect children in cyberspace.

2. International Journal of Sociology and Anthropology.
3. International Journal of Emerging Trend & Technology in Computer Science.
4. International Journal in Multidisciplinary and Academic Research.
5. National University of Juridical Sciences Law Review.
6. University of Petroleum and Energy Studies Review.
7. Book Review of Cyber Criminology.
8. Punjab University Law Review.
9. Indian Bar Review.
10. All India Reporter.
11. Journal of Business Law.
12. Journal of Criminal Law & criminology.

NEWS REPORTS

1. The Times of India.
2. The Hindu.
3. The Hindustan Times.
4. The Indian Express.

WEBSITES

1. http://www.aaets.org
2. https://www.studyinternational.com/news/cyberbullying-rampant-among-indian-students-europe-study/.
3. https://www.getsafeonline.org/socialnetworking/social-networking-sites
4. https://en.wikipedia.org/wiki/Cybercrime.
5. http://www.naavi.org/pati/pati_cybercrimes_dec03.htm
6. https://shodhganga.inflibnet.ac.in/handle/10603/2477
7. https://shodhganga.inflibnet.ac.in/handle/106/248290

Dr. Anupam Mandas
Assistant Prof. Law

Student
Sanjeev Kumar
H14109